FRSECURE
INFORMATION SECURITY EXPERTS

INFORMATION SECURITY NEWS ROUNDUP: SEPTEMBER 2017

BLOG, INFORMATION SECURITY

There was a lot of important information security news coming out of the industry during the month of September, including: The Equifax breach, North Korean cryptocurrency targeting, and more. Here are just a few of the news highlights from last month that we think you need to know about. Leave your thoughts on these, and other Information Security news stories, in the comments section.

Breaches

- Deloitte [https://www.theguardian.com/business/2017/sep/25/deloit hit-by-cyber-attack-revealing-clients-secret-emails] , one of the worlds "Big Four" accounting firms, was the victim of a sophisticated hack that allowed hackers to access confidential emails and data on some of their blue-chip clients. Hackers were able to access the global email server through an administrator's account that gave them unrestricted access. The account only asked for one password. This is another example of why two-factor authentication [https://frsecure.com/blog/what-authentication-means-in-information-security/] should be required by all organizations.
- The Securities and Exchange Commission [https://www.washingtonpost.com/amphtml/news/business reveals-it-was-hacked-information-may-have-been-used-for-illegal-stock-trades/] revealed that it was hacked. Confidential documents that had been filed by publicly traded companies was compromised in the hack. This information could have been used to make illegal trades on the market. An investigation into the matter is ongoing.
- Popular social media site, Instagram, was hacked [https://www.bankinfosecurity.com/instagram-warns-hack-more-widespread-than-expected-a-10256?rf=2017-09-06_ENEWS_SUB_BIS_Slot1&mkt_tok=eyJpIjoiWVRnMllUQmx(. Email addresses and phone numbers associated with hundreds of well known cele Emma Watson, Harry Styles, and er o dark web.

- Do you have a credit report? [https://www.consumer.gov/articles/1009-your-credit-history] If you answered yes, there's a good chance that you're among the 143 million American consumers whose personal information was exposed in the breach at Equifax. [https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do]
- The hack ran from mid-May until the breach was discovered on July 29th. [https://www.databreachtoday.com/equifax-breach-exposed-data-143-million-consumers-a-10275] This was a long enough time period for hackers to accrue millions of names, Social Security numbers, birth dates, addresses, drivers license numbers, basically everything you would need to impersonate someone.
- Equifax's response to the breach was…less than adequate, as was reported by many news outlets. [https://www.cnbc.com/2017/09/08/equifax-response-to-data-breach-leaves-many-consumers-confused.html] There were many, many things that they could have done differently once the breach was discovered. [https://frsecure.com/blog/expert-take-on-equifax-breach/]
- In the end, people were let go [https://frsecure.com/blog/what-makes-a-good-chief-security-officer/], Equifax apologized profusely [https://www.wsj.com/articles/on-behalf-of-equifax-im-sorry-1506547253], lawsuits were filed [http://money.cnn.com/2017/09/19/technology/equifax-legal-issues/index.html], and Congressional hearings took place [https://www.wired.com/story/equifax-ceo-congress-testimony/].

- The silver lining, if there is any, is that this massive breach served as a wake up call for many businesses [http://www.insidecounsel.com/2017/09/26/the-equifax-breach-wake-up-call-for-businesses] and reinforced what we have been saying here at FRSecure. [https://frsecure.com/blog/10-security-principles-live-or-die-by/]

World News

- The government of North Korea [https://www.bankinfosecurity.com/report-north-korea-seeks-bitcoins-to-bypass-sanctions-a-10293?rf=2017-09-15_ENEWS_SUB_BIS_Slot1&mkt_tok=eyJpIjoiWkdNd1l6TXhZ has turned to Bitcoin to fund its regime. North Korean agents have focused efforts on Bitcoin exchange heists and cryptocurrency mining in order to secure funds to fuel the government. As United Nation sanctions limit sources of income for North Korea, Bitcoin and other cryptocurrencies have become a way for the government to fill their pockets.
- The Department of Homeland Security ordered federal agencies and departments to remove software sold by the Russia-based IT firm Kaspersky Lab [https://www.cbsnews.com/news/dhs-bans-kaspersky-lab-software-citing-ties-to-russian-government/]. DHS cited the cybersecurity company's ties to the Russian government as rationale for the decision.

Policy/Legal News

- The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology

on-mitigating-ransomware-threats/article/687317/] to help organizations that have been affected by a ransomware attack. The guide is designed to help organizations recover data, facilitate smooth recovery in the event of a compromise, and manage risk. If all the recent breaches have taught us anything it is that no organization, no matter how big or small, should be without a Disaster Recovery Plan. [https://frsecure.com/blog/organization-big-enough-need-disaster-recovery-plan/]

- The Senate of the state of Massachusetts has established a special committee on cybersecurity [https://www.natlawreview.com/article/massachusetts-lawmakers-turn-attention-to-cybersecurity] as focus grows on improving cybersecurity policies. The Senate approved the creation of a special committee to review and improve upon the state's existing cybersecurity policies. Several bills focused on cybersecurity are pending in the state legislature.
- The Department of Homeland Security published a new rule in the Federal Register [https://www.federalregister.gov/documents/2017/09/18/2019365/privacy-act-of-1974-system-of-records] , saying it wants to include social media data as part immigration files. The new requirement is set to take effect on October 18th. Proponents of the policy [https://www.buzzfeed.com/adolfoflores/people-are-worried-about-dhs-plans-to-gather-social-media?utm_term=.arJBJqLwW#.xaxvOzja9] say that studying immigrants social media behavior could help identify possible radicals and prevent an attack on American soil while detractors claim the rule infringes on free speech rights and is just plain ineffective.

That is all for the Information Security News Recap for the month of September. Want to get more information security news? Check out FRSecure's Twitter feed [https://twitter.com/FRSecure] for updates on what's going on in the world of information security.

[https://www.linkedin.com/in/stevemarsden01/]
Steve Marsden
[https://frsecure.com/blog/author/steve-marsden/]

Senior Sales Consultant at FRSecure LLC [https://frsecure.com/]

Steve is nearly a 28 year professional sales representative who officially joined FRSecure in January, 2012 as employee number three. Steve strives to serve every customer as if they were the only; aiming for 100% customer satisfaction. An avid news junky, in his spare time Steve likes to catch up on current events, visit some Minnesota lakes, go boating, and hide in his hammock with a good book.

OCTOBER 13, 2017 / 1 COMMENT / BY STEVE MARSDEN

TAGS: INFORMATION SECURITY, INFORMATION SECURITY

You might also like

What Auther Means in Inform Securit


Inform Securit How I Went from Trainir To Trainir ...And you can too!

Securit – Back to the Basics Series - Part 3


10 Securit Princip To Live (or Die) By

Build From the Groun Up: Differe Betwee Policie Standa Proced and Guidel


Inform Securit Life Cycle, not Inform Securit Project


An Inform Securit Expert Take On The Equifa Breach


HITRU 101: Is HITRU Right for You?

1

REPLY

James

October 17, 2017 at 1:57 pm

Wow. Clearly we have not figured out how to protect our organizations. The information security industry is broken. Who will fix it?

Reply